

# KING & SPALDING

King & Spalding LLP  
1180 Peachtree Street N.E.  
Atlanta, Georgia 30309-3521  
www.kslaw.com

Phyllis B. Sumner  
Direct Dial: 404-572-4799  
Direct Fax: 404-572-5138  
psumner@kslaw.com

January 26, 2018

**RECEIVED**

**To: Exhibit A; Distribution List**

**Re: Data Security Incident**

JAN 30 2018

Referred to CPAT/IPB  
Answered \_\_\_\_\_

Dear Sir or Madam:

I write on behalf of Equifax Consumer Services LLC ("ECS") regarding the use of stolen credentials to access the accounts of 36 users of our Credit Watch service. The source of those stolen credentials is unknown. Equifax has investigated this issue as set forth below.

Based on ECS's investigation, ECS believes that the unauthorized actor(s) used stolen credentials to log into the Credit Watch accounts of 36 individuals between August 1 and September 2, 2017. Once able to log into the individual's account, the unauthorized actor(s) could potentially access profile information, including email address, phone number, user name, masked password, secret question, and secret answer. For 14 individuals, the unauthorized actor(s) also may have accessed or acquired a credit report, which contained the following data elements: full name, date of birth, last four digits of social security number, current address, former addresses, masked financial account numbers with the last four digits of the account number redacted, and other information related to the credit report, including inquiry information. There is no evidence that the unauthorized actor(s) modified any profile information for the affected individuals.

Based on the investigation, ECS has found no evidence that the above-described use of stolen credentials is related in any way to the cybersecurity incident announced by Equifax, Inc. on September 7, 2017. In addition, there is no evidence that the unauthorized actor(s) obtained the Credit Watch credentials at issue here as part of the data accessed during the incident announced on Sept. 7 or from ECS. Rather, it appears the unauthorized actor(s) obtained the Credit Watch credentials from another source and then utilized them to access the affected individuals' accounts. In addition to working with law enforcement regarding this incident, enhancements to network monitoring capabilities to detect potentially fraudulent activity are being implemented.

ECS is offering ID Patrol, a credit monitoring and identity theft protection product, at no cost for one year to the potentially affected customers. Additionally, ECS has provided affected individuals with the phone number for its call center that will be able to answer questions and provide information related to these incidents.

January 26, 2018

Page 2

Beginning on January 29, 2018, ECS will send notifications to the affected customers to explain the incident and identify steps they can take to protect themselves from identity theft. An unaddressed copy of this notification is enclosed for your reference. This notification includes information regarding the identity theft protection product that ECS is offering to potentially impacted customers. A summary table of the potentially impacted consumers by state is also attached for your reference.

Sincerely,

A handwritten signature in blue ink, appearing to read "Phyllis B. Sumner", with a long horizontal flourish extending to the right.

Phyllis B. Sumner

Enclosure

### Affected Residents By State

State	Number of Affected Residents
Arizona	2
California	8
Florida	4
Illinois	1
Louisiana	1
Maryland	2
Michigan	2
New York	1
Ohio	1
Oregon	2
Pennsylvania	2
South Carolina	1
South Dakota	1
Texas	6
Washington	2

January 29, 2018

NAME  
ADDRESS  
CITY, STATE, ZIP

**RE: Notice of Security Incident**

Dear \_\_\_\_\_:

We are writing to tell you about a data security incident that may have resulted in unauthorized access to your personal information. We take the protection and proper use of your information very seriously. For this reason, we are contacting you directly to explain the circumstances of the incident.

**What Happened**

Between August 1 and September 2, 2017, an unauthorized actor(s) obtained access to your Equifax Consumer Services LLC ("ECS") Credit Watch account. It appears that the unauthorized actor(s) used stolen credentials, the source of which is unknown, to log into your Credit Watch account. There is no evidence that the credentials used to access your account were acquired at Equifax, Inc. ("Equifax"). Upon learning of the unauthorized access, ECS promptly took steps to understand what happened, and determined that the unauthorized actor was able to access information related to your Credit Watch account and those of approximately 35 other individuals. There is no evidence that the unauthorized actor(s) modified any information related to the Credit Watch accounts.

**What Information Was Involved**

An unauthorized actor(s) may have accessed profile information relating to your Credit Watch account using stolen credentials, including email address, phone number, user name, masked password, secret question, and secret answer. [There is no evidence that the unauthorized actor(s) accessed your credit report.] [The unauthorized actor(s) also may have accessed your credit report, which contains the following information: full name, date of birth, last four digits of Social Security number, current address, former addresses, financial account numbers with the last four digits of the account number redacted, and other information related to the credit report, including inquiry information.]

This incident is unrelated to the security incident announced by Equifax on September 7, 2017.

**What We Are Doing**

Upon learning of this incident, ECS took steps to stop the access and investigate the intrusion. For your protection, ECS has locked your Credit Watch account. To unlock your account, please

visit the Credit Watch website and follow the instructions provided; when you attempt to access your account you will be asked to provide documentation, including a government issued ID, proving your identity. Enhancements to network monitoring capabilities to detect potentially fraudulent activity are being implemented.

In addition, ECS is offering you one (1) year of **ID Patrol** identity protection service at no cost to you. More information about this service is attached. To take advantage of this service, please follow the instructions in these materials between **January 29** and **April 29, 2018**.

### **What You Can Do**

Because your Credit Watch login credentials were used by an unauthorized actor(s) to access your account, and the source of the stolen credentials is unknown, if you used the same password, secret question, or secret answer for other services, we strongly recommend that you change your password, secret question, and secret answer for those other services.

Additionally, we urge you to enroll in the free identity protection service being provided by ECS.

### **For More Information**

If you have additional questions, please call our call center at 866-820-9010, available from 7:00 a.m. to 1:00 a.m. Eastern time, seven days a week. Si usted tiene preguntas, por favor llama nuestro centro de llamadas que está abierto durante los siete días de la semana desde las 7:00 a.m. hasta 1:00 a.m. hora de la costa este: 866-820-9010.

Sincerely,

Equifax Consumer Services LLC

### **Equifax ID Patrol Sign-up Steps**

ID Patrol will provide you with an "early warning system" that alerts you to changes to your credit file and help you to understand the content of your credit file at the three major credit-reporting agencies.

ID Patrol provides you with the following key features and benefits:

- Comprehensive credit file monitoring and automated alerts of key changes to your Equifax, Experian, and TransUnion credit reports
- Wireless alerts and customizable alerts available
- One 3-in-1 Credit Report and access to your Equifax Credit Report™
- Ability to receive alerts if your Social Security Number or credit card numbers are found on Internet trading sites (available online only)
- Ability to lock and unlock your Equifax Credit Report
- Up to \$1 million in identity theft insurance with \$0 deductible

Please visit [www.myservices.equifax.com/patrol](http://www.myservices.equifax.com/patrol) for more information and to enroll in ID Patrol.

Your activation code is **XXXXXX** and is valid starting January 29 and April 29, 2018 and is non-transferable.

Coverage under ID Patrol will expire 12 months from the date you activate your code by enrolling in ID Patrol online.

#### **ENROLLMENT TIPS:**

1. Use the link above to access your custom ID Patrol Enrollment page (**your activation code will NOT work if you use a different link!**)
2. Enter the Activation Code provided at the top of this page in the "Activation Code" box and click the "Submit" button.
3. The platform will walk you through the enrollment; enter the information requested, and click the "Continue" button to step through the account setup screens.
4. The system will then ask you up to four security questions to verify your identity. Please answer the questions and click the "Submit Order" button.
5. You will see an order confirmation page and you can click "View My Product" to access the product features.
6. You will receive a confirmation email.

Once enrolled, your ID Patrol comes with 24/7 live agent Customer Service (877-474-8273) to assist you in understanding the content of your Equifax credit information, provide personalized identity-theft victim assistance, and initiate an investigation of inaccurate information.

### **Identity Theft Prevention Tips**

We recommend that you remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your credit reports. You may obtain a free copy of your credit report from each company listed below once every 12 months by requesting your report online at [www.annualcreditreport.com](http://www.annualcreditreport.com), calling toll-free 1-877-322-8228, or mailing an Annual Credit Report Request Form (available at [www.annualcreditreport.com](http://www.annualcreditreport.com)) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting any of the credit reporting agencies below:

Equifax  
PO Box 740241  
Atlanta, GA 30374  
[www.equifax.com](http://www.equifax.com)  
888-766-0008

Experian  
PO Box 9554  
Allen, TX 75013  
[www.experian.com](http://www.experian.com)  
888-397-3742

TransUnion  
PO Box 2000  
Chester, PA 19016  
[www.transunion.com](http://www.transunion.com)  
800-680-7289

If you believe you are the victim of identity theft, you should contact the proper law enforcement authorities, including local law enforcement, and you should consider contacting your state attorney general and/or the Federal Trade Commission ("FTC"). You also may contact the FTC to obtain additional information about avoiding identity theft.

**Federal Trade Commission**, Consumer Response Center  
600 Pennsylvania Avenue NW, Washington, DC 20580; 1-877-IDTHEFT (438-4338)  
[www.ftc.gov/idtheft](http://www.ftc.gov/idtheft)

**State Attorneys General:** Information on how to contact your state attorney general may be found at [www.naag.org/naag/attorneys-general/whos-my-ag.php](http://www.naag.org/naag/attorneys-general/whos-my-ag.php).

You may obtain information from the FTC and the credit reporting agencies listed above about placing a fraud alert and/or credit freeze on your credit report.

**If you are a resident of Maryland**, you may obtain information about avoiding identity theft from the Maryland Attorney General's Office. This office can be reached at:

**Office of the State of Maryland Attorney General**  
200 St. Paul Place, Baltimore, MD 21202; 1-888-743-0023  
[www.marylandattorneygeneral.gov](http://www.marylandattorneygeneral.gov)

**If you are a resident of Oregon**, you may contact the Oregon Attorney General's Office at 1162 Court Street NE, Salem, OR 97301-4096, <http://www.doj.state.or.us>, (877) 877-9392 (toll-free in Oregon) or (503) 378-4400.

**Exhibit A - Distribution List**

Mark Brnovich Office of the Arizona Attorney General 1275 West Washington Street Phoenix, AZ 85007-2926 AGInfo@azag.gov	Xavier Becerra Office of the California Attorney General California Department of Justice P.O. Box 944255 Sacramento, CA 94244-2550
Pam Bondi Office of the Attorney General of Florida State of Florida The Capitol PL-01 Tallahassee, FL 32399-1050	Lisa Madigan Illinois Attorney General's Office 100 W. Randolph Street Chicago, IL 60601 databreach@atg.state.il.us
Jeff Landry Office of the Louisiana Attorney General Consumer Protection Section 1885 N. Third Street Baton Rouge, LA 70802 ConsumerInfo@ag.louisiana.gov	Brian E. Frosh Office of the Maryland Attorney General 200 St. Paul Place Baltimore, MD 21202-2202 Idtheft@oag.state.md.us
Bill Schuette Michigan Department of Attorney General 525 W. Ottawa St. P.O. Box 30212 Lansing, MI 48909 miag@michigan.gov	Eric T. Schneiderman Office of the New York Attorney General The Capitol Albany, NY 12224-0341
Mike DeWine Ohio Attorney General's Office 30 E. Broad Street, 14th Floor Columbus, OH 43215	Ellen F. Rosenblum Office of the Oregon Attorney General Oregon Department of Justice 1162 Court Street, NE Salem, OR 97301-4096
Josh Shapiro Pennsylvania Office of Attorney General 16th Floor, Strawberry Square Harrisburg, PA 17120	Alan Wilson Office of the South Carolina Attorney General P.O. Box 11549 Columbia, SC 29211
Marty J. Jackley South Dakota Attorney General's Office 1302 East Highway 14, Suite 1 Pierre, SD 57501-8501 consumerhelp@state.sd.us	Ken Paxton Office of the Texas Attorney General P.O. Box 12548 Austin, TX 78711-2548
Bob Ferguson Washington State Office of the Attorney General 1125 Washington St SE P.O. Box 40100 Olympia, WA 98504-0100 SecurityBreach@atg.wa.gov	



# KING & SPALDING

## RECEIVED

OCT 20 2017

Referred to

*CPAT/PB*

Answered

October 12, 2017

King & Spalding LLP  
1180 Peachtree Street N.E.  
Atlanta, GA 30309-3521  
Tel: +1 404 572 4600  
Fax: +1 404 572 5100  
www.kslaw.com

Phyllis B. Sumner  
Direct Dial: +1 404 572 4799  
Direct Fax: +1 404 572 5100  
psumner@kslaw.com

To: Exhibit A; Distribution List

Re: Data Security Incident Announced on September 7, 2017 Affecting Equifax Inc.

Dear Sir or Madam,

I write on behalf of Equifax Inc. ("Equifax") to follow up on the September 7, 2017 notification regarding a cybersecurity incident impacting the personal information of U.S. consumers. On October 2, 2017, Equifax announced that the cybersecurity firm Mandiant completed the forensic portion of its investigation of the cybersecurity incident announced on September 7, 2017 to finalize the consumers potentially impacted. The completed review determined that approximately 2.5 million additional U.S. consumers were potentially impacted, for a total of approximately 145.5 million. An updated approximate number of potentially impacted residents in your state is identified in Exhibit B.

Mandiant did not identify any evidence of additional or new attacker activity or any access to new databases or tables. Instead, this additional population of consumers was confirmed during Mandiant's completion of the remaining investigative tasks and quality assurance procedures built into the investigative process. To be clear, additional U.S. consumers identified, and the unauthorized access of information, all relate to the cybersecurity incident disclosed on September 7, 2017. To minimize confusion, Equifax will mail written notices to all of the additional potentially impacted U.S. consumers identified since the September 7 announcement. An unaddressed copy of that letter is attached as Exhibit C. The feature on the dedicated website, [www.equifaxsecurity2017.com](http://www.equifaxsecurity2017.com), that U.S. consumers may use to determine whether they may have been impacted has been updated to reflect the additional 2.5 million impacted U.S. consumers. Equifax takes seriously its responsibility to protect the security of personal information, and our priority is to assist consumers who may have been impacted.

Please do not hesitate to contact me if you have any questions regarding this update.

Sincerely,



Phyllis B. Sumner

CC: Zachary Fardon  
Christopher C. Burris

Enclosures

### **Exhibit A - Distribution List**

Steve Marshall Office of the Alabama Attorney General Office of the Attorney General P.O. Box 300152 Montgomery, AL 36130-0152	Jahna Lindemuth Alaska Attorney General Office 1031 West 4th Avenue, Suite 200 Anchorage, AK 99501 attorney.general@alaska.gov
Mark Brnovich Office of the Arizona Attorney General 1275 West Washington Street Phoenix, AZ 85007-2926 AGInfo@azag.gov	Leslie Rutledge Arkansas Attorney General Office 323 Center Street, Suite 200 Little Rock, AR 72201 oag@ArkansasAG.gov
Xavier Becerra Office of the California Attorney General California Department of Justice P.O. Box 944255 Sacramento, CA 94244-2550	Cynthia H. Coffman Office of the Colorado Attorney General Colorado Department of Law Ralph L. Carr Judicial Building 1300 Broadway, 10th Floor Denver, CO 80203
George Jepsen State of Connecticut Attorney General's Office 55 Elm Street Hartford, CT 06106 ag.breach@ct.gov	Karl A. Racine District of Columbia Attorney General 441 4th Street, NW Washington, DC 20001 dc.oag@dc.gov
Matt Denn Delaware Attorney General Delaware Department of Justice Carvel State Building 820 N. French St. Wilmington, DE 19801 attorney.general@state.de.us	Pam Bondi Office of the Attorney General of Florida State of Florida The Capitol PL-01 Tallahassee, FL 32399-1050
Chris Carr Office of the Georgia Attorney General 40 Capitol Square, SW Atlanta, GA 30334	Douglas Chin Department of the Attorney General of Hawaii 425 Queen Street Honolulu, HI 96813

<p>Hawaii Office of Consumer Protection  Leiopapa A Kamehameha Building aka State  Office Tower  235 South Beretania Street  Honolulu, Hawaii 96813  dcca@dcca.hawaii.gov</p>	<p>Lawrence Wasden  State of Idaho Attorney General's Office  700 W Jefferson St., Suite 210  P.O. Box 83720  Boise, ID 83720-0010</p>
<p>Lisa Madigan  Illinois Attorney General's Office  100 W. Randolph Street  Chicago, IL 60601  databreach@atg.state.il.us</p>	<p>Curtis T. Hill, Jr.  Indiana Attorney General's Office  Indiana Government Center South  302 W. Washington St., 5th Floor  Indianapolis, IN 46204  IDTheft@atg.in.gov</p>
<p>Tom Miller  Office of the Attorney General of Iowa  Hoover State Office Bldg.  1305 E. Walnut Street  Des Moines, IA 50319  consumer@iowa.gov</p>	<p>Derek Schmidt  Kansas Attorney General  120 S.W. 10th Ave., 2nd Floor  Topeka, KS 66612-1597</p>
<p>Andy Beshear  Office of the Kentucky Attorney General  700 Capitol Ave, Suite 118  Frankfort, KY 40601-3449</p>	<p>Jeff Landry  Office of the Louisiana Attorney General  P.O. Box 94005  Baton Rouge, LA 70804-4095  ConsumerInfo@ag.louisiana.gov</p>
<p>Janet T. Mills  Office of the Maine Attorney General  6 State House Station  Augusta, ME 04333  breach.security@maine.gov</p>	<p>Brian E. Frosh  Office of the Maryland Attorney General  200 St. Paul Place  Baltimore, MD 21202-2202  Idtheft@oag.state.md.us</p>
<p>Maura Healey  Office of the Attorney General of  Massachusetts  One Ashburton Place  Boston, MA 02108-1518  ago@state.ma.us</p>	<p>Bill Schuette  Michigan Department of Attorney General  525 W. Ottawa St.  P.O. Box 30212  Lansing, MI 48909  miag@michigan.gov</p>
<p>Lori Swanson  Office of the Minnesota Attorney General  445 Minnesota Street, Suite 1400  St. Paul, MN 55101-2131  Attorney.General@ag.state.mn.us</p>	<p>Jim Hood  Mississippi Attorney General's Office  550 High Street  Jackson, MS 39201</p>

<p>Josh Hawley Missouri Attorney General's Office Supreme Court Building 207 W. High St. P.O. Box 899 Jefferson City, MO 65102 attorney.general@ago.mo.gov</p>	<p>Tim Fox Office of the Montana Attorney General Justice Building, Third Floor 215 North Sanders P.O. Box 201401 Helena, MT 59620-1401 contactdoj@mt.gov</p>
<p>Montana Office of Consumer Protection P. O. Box 200151 Helena, MT 59620-0151 contactocp@mt.gov</p>	<p>Doug Peterson Nebraska Attorney General's Office 2115 State Capitol P.O. Box 98920 Lincoln, NE 68509 ago.consumer@nebraska.gov</p>
<p>Adam Paul Laxalt Office of the Nevada Attorney General 100 North Carson Street Carson City, NV 89701 AgInfo@ag.nv.gov</p>	<p>Gordon J. MacDonald New Hampshire Department of Justice 33 Capitol Street Concord, NH 03301 attorneygeneral@doj.nh.gov</p>
<p>Christopher S. Porrino Office of the New Jersey Attorney General RJ Hughes Justice Complex 25 Market Street, Box 080 Trenton, NJ 08625-0080 databreach@cyber.nj.gov</p>	<p>Hector Balderas Office of the New Mexico Attorney General 408 Galisteo Street Villagra Building Santa Fe, NM 87501</p>
<p>Eric T. Schneiderman Office of the New York Attorney General The Capitol Albany, NY 12224-0341</p>	<p>Josh Stein North Carolina Attorney General's Office 9001 Mail Service Center Raleigh, NC 27699-9001</p>
<p>Wayne Stenehjem North Dakota Attorney General's Office 600 E. Boulevard Ave. Dept. 125 Bismarck, ND 58505 ndag@nd.gov</p>	<p>Mike DeWine Ohio Attorney General's Office 30 E. Broad Street, 14th Floor Columbus, OH 43215</p>
<p>Mike Hunter Oklahoma Office of the Attorney General 313 NE 21st Street Oklahoma City, OK 73105</p>	<p>Ellen F. Rosenblum Office of the Oregon Attorney General Oregon Department of Justice 1162 Court Street, NE Salem, OR 97301-4096</p>

<p>Josh Shapiro  Pennsylvania Office of Attorney General  16th Floor, Strawberry Square  Harrisburg, PA 17120</p>	<p>Puerto Rico Departamento de Asuntos del Consumidor  Ave. José De Diego, Pda. 22  Centro Gubernamental Minillas  Edificio Torre Norte, Piso 7  San Juan, PR 00940  servicio@daco.pr.gov</p>
<p>Peter F. Kilmartin  Office of the Rhode Island Attorney General  150 South Main Street  Providence, RI 02903</p>	<p>Alan Wilson  Office of the South Carolina Attorney General  P.O. Box 11549  Columbia, SC 29211</p>
<p>Consumer Protection Division of the Department of Consumer Affairs  P.O. Box 5757  Columbia, SC 29250</p>	<p>Marty J. Jackley  South Dakota Attorney General's Office  1302 East Highway 14, Suite 1  Pierre, SD 57501-8501  consumerhelp@state.sd.us</p>
<p>Herbert H. Slatery, III  Office of the Tennessee Attorney General and Reporter  P.O. Box 20207  Nashville, TN 37202-0207</p>	<p>Ken Paxton  Office of the Texas Attorney General  P.O. Box 12548  Austin, TX 78711-2548</p>
<p>Sean D. Reyes  Utah Office of the Attorney General  Utah State Capitol Complex  350 N. State St., Suite 230  Salt Lake City, UT 84114-2320  uag@agutah.gov</p>	<p>TJ Donovan  Vermont Attorney General's Office  109 State Street  Montpelier, VT 05609-1001  ago.cap@vermont.gov</p>
<p>Mark R. Herring  Office of the Virginia Attorney General  202 North Ninth Street  Richmond, VA 23219</p>	<p>Bob Ferguson  Washington State Office of the Attorney General  1125 Washington St SE  P.O. Box 40100  Olympia, WA 98504-0100  SecurityBreach@atg.wa.gov</p>

Patrick Morrissey Office of the West Virginia Attorney General State Capitol Complex Bldg. 1, Room E-26 Charleston, WV 25305 consumer@wvago.gov	Brad Schimel Office of the Wisconsin Attorney General Wisconsin Department of Justice P.O. Box 7857 Madison, WI 53707-7857
Peter K. Michael Wyoming Attorney General's Office Kendrick Building 2320 Capitol Avenue Cheyenne, WY 82002 ag.consumer@wyo.gov	

**Exhibit B – Approximate Number of Potentially Impacted Residents**

**Updated: October 12, 2017**

South Carolina – Approximately 2,419,033

## Exhibit C





P.O. Box 105054  
Atlanta, GA 30348

Name  
Street  
City, State Zip

October 13, 2017

## NOTICE OF DATA BREACH

Dear Customer:

This letter follows up on the cybersecurity incident Equifax announced on September 7, 2017. At Equifax, our priorities with regard to this incident are transparency and continuing to provide timely, reassuring support to every consumer. You are receiving this letter because you are one of the 2.5 million additional potentially impacted U.S. consumers that has personal information that was potentially exposed, as described below.

### **What Happened**

On July 29, 2017, Equifax discovered that criminals exploited a U.S. website application vulnerability to gain access to certain files. Upon discovery, we acted immediately to stop the intrusion. The company promptly engaged a leading, independent cybersecurity firm which has been conducting a comprehensive forensic review to determine the scope of the intrusion, including the specific data impacted. Equifax also reported the criminal access to law enforcement and continues to work with authorities. Based on the company's investigation, the unauthorized access occurred from mid-May through July 2017.

On September 7, 2017 Equifax notified U.S. consumers of the data security incident, including that approximately 143 million U.S. consumers were impacted. On October 2, 2017, following the completion of the forensic portion of the investigation of the incident, Equifax announced that the review determined that approximately 2.5 million additional U.S. consumers were potentially impacted. To minimize confusion, you are receiving this letter because you are one of the 2.5 million additional potentially impacted U.S. consumers.

### **What Information Was Involved**

Most of the consumer information accessed includes names, Social Security numbers, birth dates, addresses, and in some instances, driver's license numbers. In addition to this notice, Equifax will send you a direct mail notice if your credit card number was impacted. We have found no evidence of unauthorized access to Equifax's core consumer or commercial credit reporting databases.

### **What We Are Doing**

Upon learning of this incident, Equifax took steps to stop the intrusion, and engaged an independent cybersecurity firm to forensically investigate and determine the scope. Equifax also engaged the cybersecurity firm to conduct an assessment and provide recommendations on steps that can be taken to help prevent this type of incident from happening again.

Equifax is focused on consumer protection and has established a dedicated website, [www.equifaxsecurity2017.com](http://www.equifaxsecurity2017.com) to help consumers. We are also offering free identity theft protection and credit file monitoring to all U.S. consumers, even if a consumer is not impacted by this incident. This offering, called TrustedID Premier, includes 3-Bureau credit monitoring of your Equifax, Experian and TransUnion credit reports; copies of your Equifax credit report; the ability to lock and unlock your Equifax credit report; identity theft insurance; and Internet scanning for your Social Security number - all complimentary to U.S. consumers for one year. To find out more information on this complimentary offer and to sign up, please click on the tab "What Can I Do" on the dedicated website. You must complete the enrollment process by January 31, 2018.

In addition, by January 31, 2018, Equifax will offer a new service allowing all consumers the option of controlling access to their personal credit data. The service we are developing will let consumers easily lock and unlock access to their Equifax credit files -- for free, for life.

### **What You Can Do**

In addition to enrolling in identity theft protection and credit file monitoring, please see the "Identity Theft Prevention Tips" and State Information below. This information provides additional steps you can take, including how to obtain a free copy of your credit report and place a fraud alert and/or credit freeze on your credit report. In addition, please monitor your account statements and report any unauthorized charges to your credit card companies and financial institutions.

### **For More Information**

Equifax is committed to ensuring that your personal information is protected, and we apologize to you for the concern and frustration this incident causes. If you have additional questions, please call our dedicated call center at 866-447-7559, available from 7:00 a.m. to 1:00 a.m. Eastern time, seven days a week. Si usted tiene preguntas, por favor llama nuestro centro de llamadas que está abierto durante los siete días de la semana desde las 7:00 a.m. hasta 1:00 a.m. hora de la costa este: 866-447-7559.

Sincerely,

Equifax Inc.

### **Identity Theft Prevention Tips**

We recommend that you remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your credit reports. You may obtain a free copy of your credit report from each company listed below once every 12 months by requesting your report online at [www.annualcreditreport.com](http://www.annualcreditreport.com), calling toll-free 1-877-322-8228, or mailing an Annual Credit Report Request Form (available at [www.annualcreditreport.com](http://www.annualcreditreport.com)) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting any of the credit reporting agencies below:

Equifax  
PO Box 740241  
Atlanta, GA 30374  
[www.equifax.com](http://www.equifax.com)  
888-766-0008

Experian  
PO Box 9554  
Allen, TX 75013  
[www.experian.com](http://www.experian.com)  
888-397-3742

TransUnion  
PO Box 2000  
Chester, PA 19016  
[www.transunion.com](http://www.transunion.com)  
800-680-7289

If you believe you are the victim of identity theft, you should contact the proper law enforcement authorities, including local law enforcement, and you should consider contacting your state attorney general and/or the Federal Trade Commission ("FTC"). You also may contact the FTC to obtain additional information about avoiding identity theft.

**Federal Trade Commission**, Consumer Response Center  
600 Pennsylvania Avenue NW, Washington, DC 20580; 1-877-IDTHEFT (438-4338)  
[www.ftc.gov/idtheft](http://www.ftc.gov/idtheft)

**State Attorneys General:** Information on how to contact your state attorney general may be found at [www.naag.org/naag/attorneys-general/whos-my-ag.php](http://www.naag.org/naag/attorneys-general/whos-my-ag.php).

You may obtain information from the FTC and the credit reporting agencies listed above about placing a fraud alert and/or credit freeze on your credit report.

### **IF YOU ARE A MARYLAND RESIDENT**

You may obtain information about avoiding identity theft from the Maryland Attorney General's Office. This office can be reached at:

**Office of the State of Maryland Attorney General**  
200 St. Paul Place Baltimore, MD 21202; 1-888-743-0023  
[www.marylandattorneygeneral.gov](http://www.marylandattorneygeneral.gov)

### **IF YOU ARE A MASSACHUSETTS RESIDENT**

Under Massachusetts law, you also have the right to obtain a police report in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it. You may also consider placing a fraud alert message or security freeze on your credit file by calling the toll-free telephone numbers for each of the three national consumer credit reporting agencies listed above. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit, mortgages, employment, housing or other services.

If you have been a victim of identity theft and you provide the credit reporting agency with a valid police report, it cannot charge you to place, lift or remove a security freeze. In all other cases, a credit reporting agency may charge you up to \$5.00 each to place, temporarily lift, or permanently remove a security freeze. To place a security freeze on your credit file, you must send a written request to **each** of the three national consumer reporting agencies listed above by regular, certified or overnight mail. In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address such as a current utility bill or telephone bill;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft;
8. If you are not a victim of identity theft, include payment by check, money order, or credit card (Visa, MasterCard, American Express or Discover only). Do not send cash through the mail.

The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password, or both, that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and social security number) **and** the PIN number or password provided to you when you placed the security freeze as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and social security number) **and** the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.

#### **IF YOU ARE A NEW MEXICO RESIDENT**

Under New Mexico law, you also have the right to obtain a police report in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it. You may also consider placing a fraud alert message or security freeze on your credit file by calling the toll-free telephone numbers for each of the three national consumer credit reporting agencies listed above. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit, mortgages, employment, housing or other services.

If you have been a victim of identity theft and you provide the credit reporting agency with a valid police

report, it cannot charge you to place, lift or remove a security freeze. Alternatively, if you are over the age of 65, then the fee will also be waived. In all other cases, a credit reporting agency may charge you up to \$10.00 each to place, temporarily lift, or permanently remove a security freeze. To place a security freeze on your credit file, you must send a written request to **each** of the three national consumer reporting agencies listed above by regular, certified or overnight mail. In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address such as a current utility bill or telephone bill;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft;
8. If you are not a victim of identity theft, include payment by check, money order, or credit card (Visa, MasterCard, American Express or Discover only). Do not send cash through the mail.

The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password, or both, that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and Social Security number) **and** the PIN number or password provided to you when you placed the security freeze as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and Social Security number) **and** the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.

#### **IF YOU ARE A NORTH CAROLINA RESIDENT**

You may obtain information about avoiding identity theft from the North Carolina Attorney General's Office. This office can be reached at:

**North Carolina Attorney General's Office**  
9001 Mail Service Center Raleigh, NC 27699-9001; 919-716-6400  
[www.ncdoj.gov](http://www.ncdoj.gov)

#### **IF YOU ARE A RHODE ISLAND RESIDENT**

You may obtain information about avoiding identity theft from the Rhode Island Attorney General's Office. This office can be reached at:

**Office of the State of Rhode Island Attorney General**  
150 South Main Street Providence, RI 02903; 401-274-4400  
www.riag.ri.gov

Under Rhode Island law, you also have the right to obtain a police report in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it. You may also consider placing a fraud alert message or security freeze on your credit file by calling the toll-free telephone numbers for each of the three national consumer credit reporting agencies listed above. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit, mortgages, employment, housing or other services.

If you have been a victim of identity theft and you provide the credit reporting agency with a valid police report, it cannot charge you to place, lift or remove a security freeze. Alternatively, if you are over the age of 65, then the fee will also be waived. In all other cases, a credit reporting agency may charge you up to \$10.00 each to place, temporarily lift, or permanently remove a security freeze. To place a security freeze on your credit file, you must send a written request to **each** of the three national consumer reporting agencies listed above by regular, certified or overnight mail. In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address such as a current utility bill or telephone bill;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft;
8. If you are not a victim of identity theft, include payment by check, money order, or credit card (Visa, MasterCard, American Express or Discover only). Do not send cash through the mail.

The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password, or both, that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and Social Security number) **and** the PIN number or password provided to you when you placed the security freeze as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and Social Security number) **and** the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.